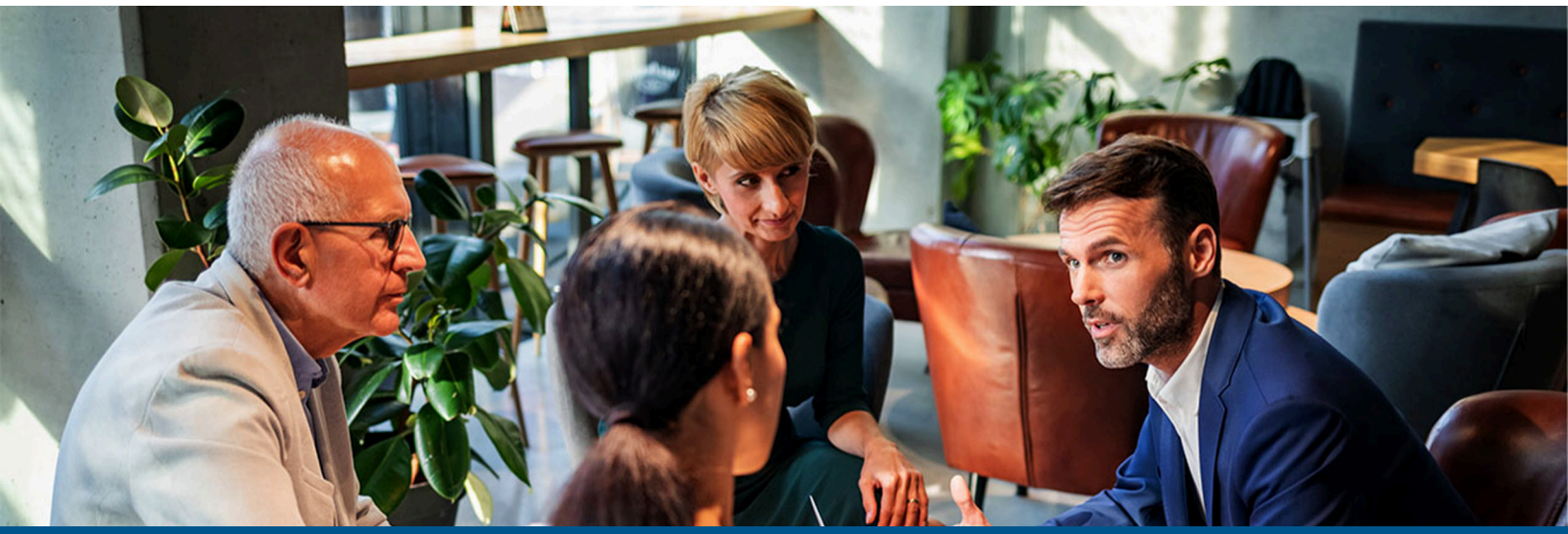


Kofax Unified Client for HP
Getting Started Guide

Version: 1.3.0

Date: 2024-04-08

KOFAX

Table of Contents

Chapter 1

Kofax Unified Client for HP

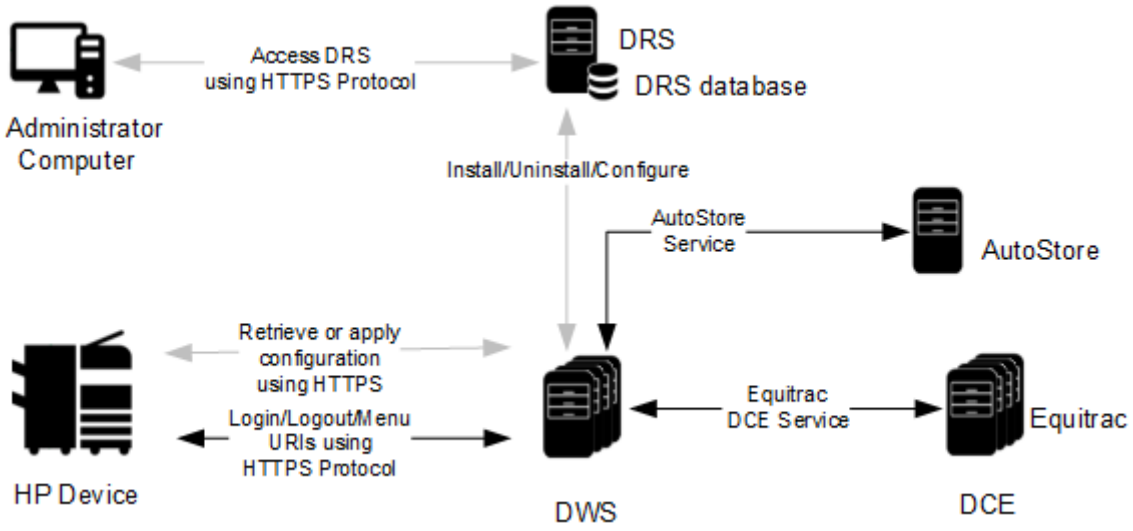
The Kofax Unified Client for HP provides a unified client for capture and print management functionality on specific HP Multi-Function Printers (MFPs), Single-Function Printers (SFPs), and Digital Sender devices. The capture (with process and route) functionality within the client is provided by Kofax AutoStore, while the print management capability is provided by Kofax Equitrac or Kofax Output Manager.

The unified client uses the Device Registration Service (DRS) to configure and deploy the embedded client to single or multiple HP devices, using one of the following server configurations:

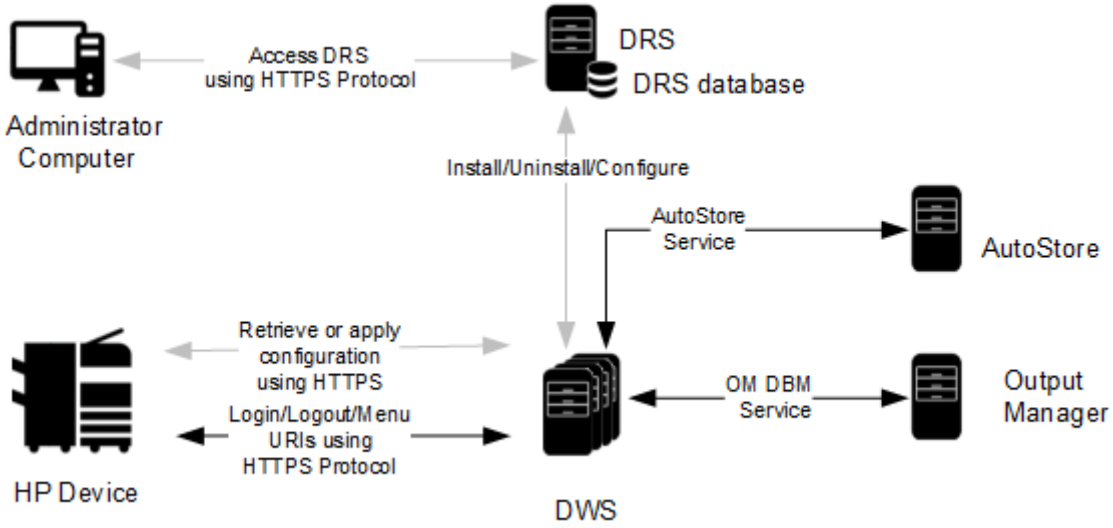
1. AutoStore and Equitrac components.
2. AutoStore and Output Manager components.
3. Equitrac component only.
4. Output Manager component only.
5. AutoStore component only.

If your HP device is an SFP, you cannot select a configuration with AutoStore as scanning is not supported.

This figure illustrates a typical architecture for a system that includes the Unified Client with Equitrac and AutoStore:



This figure illustrates a typical architecture for a system that includes the Unified Client with Output Manager and AutoStore:



The Unified Client provides device authentication and optional authorization to securely access the device. It provides a single application for Kofax print and capture workflows.

When deployed to the HP device with Equitrac or Output Manager, the Unified Client controls access to the device and acts as the gateway for Kofax functionality. Users must authenticate to gain access to Kofax-controlled device functions. In this case, the client allows users to select functions, such as Print-to-Me and scanning, from a common Kofax Launcher screen (where users can start the available workflows), provides card reader support, searchable billing codes at device login, and job accounting. It supports Equitrac authentication through user name, password, and card swipe with an optional PIN.

When deployed to the HP device with AutoStore only, the client does not control access to the device and provides capture workflows from a Kofax Launcher screen.

The Unified Client supports DWS and DCE failover. You can specify up to three additional DWS servers and DCE servers to ensure that the HP device continues to function for users if your primary DWS or DCE is offline.

On HP devices, users might need to press the **Reset** button if they are in front of the device during a DWS or DCE transition to ensure that the device is displaying the correct Unified Client user interface.

Chapter 2

Before you begin

Prerequisites

Before you begin, ensure that the following requirements are met.

Use the following links to view the technical specifications and minimum requirements for each of the ControlSuite components. Specific requirements depend on the number of servers in a deployment, operating systems, expected production volume, and other applications in the environment.

- AutoStore
- Equitrac
- Output Manager
- DRS
- DWS

Check	Description
☐	Verify that your device is supported. For the latest list of supported HP models, consult your local HP representative or refer to the Kofax Supported Devices web page.
☐	Verify that the server machine is a member of a domain.
☐	Verify that you have Administrative access rights to Windows on the server.
☐	Check that all important Windows updates are installed.
☐	Verify that Microsoft Windows Updates is turned on if you are deploying AutoStore. This is necessary for the successful installation of Microsoft Windows Identity Foundation (TFS).
☐	Ensure that Windows Identity Foundation 3.5 is installed on the server: launch **Server Manager** > **Local Server** , and confirm that Windows Identity Foundation 3.5 is listed under Roles and Features.
☐	Verify that IE Enhanced Security Configuration is turned off for Administrators in **Server Manager** > **Local Server** > **IE Enhanced Security Configuration** .
☐	Verify that you have Administrative access to the HP device.
☐	Check that your servers and HP devices have a DNS record.

DRS and unified client communication ports

The following table provides general information on ports and protocols for the DRS server and the Unified Client for HP.

Component	Device display menu protocol	Device file transport protocol	Default communication port	Port configurable	Required device components
DRS server	HTTP, HTTPS	HTTP, HTTPS	Web server: 8753 REST-based web service: 8755 Client Server: 9000 Web client: 9000	Yes	
Unified Client for HP	See Default communication port.	See Default communication port.	AutoStore application port (http/https): - AutoStore server: 3310 (DWS to AutoStore) Output Manager application port (http/https): - 8069 DWS (https) - 8444 (Device to DWS)	Yes	DWS source ports chosen by the operating system are usually ports 61555 and above. These ports must be opened for outbound traffic.
			Equitrac application port (http/https): - 2939 (DWS to Equitrac) Device port for HTTPS communications: - 443 (DWS to device) HP device services (https): - 7627 (DWS to device) HP device discovery tree (http): - 80 (DWS to device)	No	

Supported card readers

The Unified Client for HP supports the following card readers.

Kofax card readers

- Kofax Micro Card Reader
- Kofax Equitrac ID Card Reader
- Kofax MX Proximity TWN4 Reports

- Kofax MX Proximity TWN4

And the Unified Client for HP allows the usage of the following card readers.

Third-party card readers

- Elatec TWN3
- Elatec TWN4
- RFIDeas pcProx RDR-7L81AKU
- RFIDeas pcProx RDR-80581AKU
- HP Universal Card Reader
- HP HIP2 Keystroke Reader
- Custom

When a third-party card reader is used, then a third-party card reader license is required.

Dual stack limitations

Dual stack environments contain a mix of IPv4 and IPv6 addresses within the same deployment. A dual stack environment has the following limitations for devices and DWS:

- You cannot mix IP addresses combinations for devices and DWS in DRS. For example, you cannot use IPv4 for devices and IPv6 for DWS.
- You cannot use IPv4 addresses for devices and host names for DWS in DRS.

Chapter 3

Configure DRS

Use DRS to configure and deploy the unified client

DRS is installed as a ControlSuite component. Administrative access to the server is required. The following steps are performed on the server where the installation takes place.

1. Open DRS. In a Web browser, enter http://<DRSServerIP>:9000/ where <DRSServerIP> is the IP address of the server where DRS is installed.
2. Create an application in DRS:
   a. Select the **Applications** tab.
   b. Click the New (⊕) button at the top left of the **Applications** pane.
   c. In the **Name** field (required), enter an application name.
   d. Select **HP Unified Client** as the **Application Type**.
   e. In the **DWS Server Address** field (required), enter the primary DWS host name. It is recommended that you use the fully qualified domain name of the server instead of the IP address. If you cannot use the fully qualified domain name, use an IPv4 address.
   f. If you have additional DWS servers for failover purposes, enter their host names in the **DWS Server #2 Address**, **DWS Server #3 Address**, and **DWS Server #4 Address** fields.
   g. In the **DWS Server(s) Port** field, enter the port number. The default is 8444.
   h. For **Trust Self-signed Certificate for DWS Server**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.
   i. In the **Server Configuration** list, select one of the following options: **AutoStore and Equitrac**, **AutoStore and Output Manager**, **Equitrac**, **Output Manager** or **AutoStore**.

      ⓘ If your HP device is a Single-Function Printer (SFP), you cannot select a configuration with AutoStore as scanning is not supported.

      Based on the server selection, only some of the following application fields are visible.
   j. If you select **AutoStore** as part of the configuration, complete the following information:
      - Enter the host name or IP address for the **AutoStore Server Address**.
      - Enter the **AutoStore Server TLS Port** number that the AutoStore server uses to communicate with the ControlSuite. By default, the port number is 3310.
      - For **AutoStore Server Use TLS**, select **True** or **False**.
      - For **Trust Self-signed Certificate for AutoStore Server**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.

k. If you select **Equitrac** as part of the configuration, complete the following information:
   - In the **DCE Server Address** field (required), enter the IP address or host name used by the Equitrac Server.
   - If you have additional DCE servers for failover purposes, enter their IP addresses in the **DCE Server #2 Address**, **DCE Server #3 Address**, and **DCE Server #4 Address** fields.
   - For **Trust Self-signed Certificate for DCE Server**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.

l. If you select **Output Manager** as part of the configuration, complete the following information:
   - In the **Print Manager Address** field, enter the IP address or host name used by the Output Manager server.
   - Enter the **Print Manager TLS Port** number. By default, the port number is 8068.
   - For **Print Manager Use TLS**, select **True** or **False**.

m. For **Authentication**, select **True** if the ControlSuite is an authentication provider on the device or **False** if authentication is completed by a third-party provider, such as CAC. This option is not available for an AutoStore only configuration.

n. For **Kofax Authorization**, select **True** to use one of the authorization profiles offered by the ControlSuite or **False** to use another authorization agent outside of the ControlSuite. This option is not available for an AutoStore only configuration.

o. Click **Save** ( ).

3. Add a device in DRS:

a. Click the **Devices** tab.

b. Click the New ( ) button at the top left of the **Devices** pane. The **Add Device** function loads into the right pane.

c. In the **Name** field (required), enter a name for the HP device or device group that identifies it on the network.

d. In the **Address** field (required), enter the address of the device. While IP addresses can be used, it is preferable to use the fully-qualified domain name. When using the hostname, ensure that the server is configured properly with the DNS server to resolve the hostname.

> You cannot specify a static IPV6 address for the device in DRS. It must be a host name or a static IPV4 address.

e. Enter the **Username** and **Password** for the device. Typically, the username is admin.

f. In the **Application** list (required), select the application you created in the previous step. The remaining device fields appear.

g. In the **Device Group** field, enter the name of the device group, if applicable.

h. For **Trust Self-signed Certificate for device**, select **False** to use certificates from a trusted certificate authority or **True** to use self-signed certificates.

i. For **Customize Application Name**, select **True** to display the **Application Name** field and enter a name for the application. This name will appear under the button on the HP device home screen that is used to access Kofax workflows.

j. For **Customized Assets**, select **True** to choose a new app icon. The **Application Icon** field appears. Enter the file name of the new icon.

> The icon size must be 72x72 in a JPEG, PNG, or BMP format.

k. If you selected **Equitrac** or **Output Manager** as the configuration, complete the following information.

- If a card reader is attached to the device, select the type from the **Card Reader Model** list. If your card reader is not listed, you can select **Custom** and enter the **PID** and **VID** of the card reader.
- In the **Authorization Level** list (required if you enabled Kofax authorization), select one of the following authorization profiles:
  - **Standard Kofax Admin Authorization**: This profile locks specific applications and features for administrators only. After logging in, users can access all other device applications.
  - **Standard Kofax User Authorization**: This profile makes all applications and features available to users after logging in.
  - **Standard Kofax Guest Authorization**: This profile makes all applications and features available to users without requiring them to log in. Some applications, such as device settings, are restricted to administrators. Access to Kofax workflows requires a user to log in using the Kofax authentication option.

For more information, see Authorization.

l. For **Customize Workflow Buttons**, select **True** if you want to display the device native apps on the Launcher screen. The **Workflow Applications** field appears. Choose the available workflow applications for your device.

m. Click **Save** ( ) at the top of the **Add Device** pane.

4. From the list at the top of the **Details** pane, select **Install and Configure**.

> The primary DWS must be online and available when installing the application.

5. Click **Run Action** ( ). This action may take a few moments to complete. Once finished, a **Successfully completed** message appears in the **Action History** pane at the bottom of the screen.

> If you want to change any settings in the application (such as the primary DWS server or server details for Equitrac or AutoStore), you must use the **Uninstall and Delete** action in to remove the application profile from the device, update the application settings, then choose the **Install and Configure** action again.

Authorization

When the authorization application setting is enabled in DRS, the Unified Client for HP offers different levels of authorization, which control how users access the applications on the device. Authorization profiles are set when applications are created or configured, then assigned at device or device group level. You can set the authorization level while creating a the Unified Client for HP application.

The following authorization profiles are available:

- **Administrator authorization**: Specific applications and features are locked for administrators only. These items are denoted with a lock icon on the device. After logging in, users can access all other device applications.
- **User authorization**: All applications and features are available to users after logging in.

  This profile allows Kofax users access to device configuration settings.

- **Guest authorization**: Users do not need to log in to use device features and applications. Some applications, such as device settings, are restricted to administrators. Applications and features that are specific to the Unified Client for HP are not available to guest users; users must always log in.

- If you want to change the authorization level in DRS, you can change it and update the application using the Update Configuration action.
- With user and guest authorization, only administrators can create or configure the HP Quick Sets or default features for Copy, Scan, or Fax.

If you do not want to enable authorization or if you remove Kofax Authorization from a device that previously had it, you need to use another service outside of the Unified Client for HP to configure access to device functions. The Unified Client must be locked to User access and the Kofax application used for login.

Chapter 4

Additional information

Product documentation

The full product documentation set for the Unified Client for HP 1.3.0 is available online at the Kofax ControlSuite 1.4.0 site. This documentation set consists of the following documentation to assist you with installing, configuring, and using the product.

- ControlSuite Clients Help, which contains help for the Unified Client for HP, DRS, and other components and clients
- ControlSuite server help, which contains help for ControlSuite installation and configuration
- Release Notes
- Technical Specifications

Troubleshooting

Issue	Cause	Solution
If your configuration includes Output Manager and you are trying to authenticate using Kofax Business Connect, you might receive a message on the HP device, "Please follow the prompts on your mobile device.", without any prompts.	Some Output Manager authentication options are not supported with Business Connect.	Turn off the following authentication options from the Output Manager Console. 1. In the Set General Preferences utility, click the **Security** tab. 2. In the **External client login** section, clear Require PIN with Card ID entry and Require PIN with card swipe

Issue	Cause	Solution
The HP device shows the following USB error: "Attached USB device will not be used because it is not supported.”	Most likely the card reader plugged in to the HP device was not correctly setup in DRS prior to installing the client	Confirm that no unauthorized USB devices are plugged in. If the message stills remains, confirm that you selected the right card reader in DRS or typed in the correct custom PID/VID, and reinstall that device if you need to change it. If using a named reader you can plug the reader in to your laptop to confirm PID/VID and use the custom entry to type it in.
You receive Web browser alerts or messages that there is a hostname mismatch.	This issue occurs when you have entered an IP address instead of a server hostname as your DWS Server Address in DRS. Your environment might require the use of IP addresses.	Dismiss the alert messages and continue using the Web browser. If supported by your environment, enter a server hostname for the DWS Server Address.
When pressing Sign In on the HP device, you might receive an error that the device “failed to verify server certificate fingerprint".	There is an invalid or duplicate root certificate for DWS installed on the HP device.	1. Log in to the HP device web administration page. 2. Go to **Security** > **Certificate Management** . 3. Delete any certificates that are issued by Kofax DWS. 4. In DRS, deploy the ControlSuite to this device again.
The HP device does not show the Kofax branded icon on the HP Home screen launcher button.	Unified Client for HP 1.1 originally used a generic icon for the launcher button. This was updated in ControlSuite 1.1 fix pack 5 to be a Kofax branded icon. However, since the icon is cached on the device, the new icon is not displayed.	Using DRS, run the install task on the devices that you want to update the new Kofax icon to.

Error messages

Registration error messages

Code	Message	Comments
400	Failed to register device with DWS.	Device errors. Contact Support for assistance.
401	Invalid credentials.	Verify that you entered the correct credentials and try logging on again.

Code	Message	Comments
402	Failed to deregister device from DWS.	Device errors. Contact Support for assistance.
403	Failed to configure DWS server.	Try again later.
505	DWS installation aborted due to licensing restrictions.	Contact Kofax Support.
506	Product has not been installed.	
507	DWS installation procedure has not completed yet, checking prerequisites.	Review the installation checklists and try again.
508	DWS server not reachable.	Try again later.
509	DWS authentication failed.	Contact Kofax Support.
510	DWS installation failed.	A device was in use or had a logged on user. Restart the device and make sure no user are logged on to the device, and there are no running scan jobs and registration processes. Then, try deploying the client again.
511	DWS certificate invalid.	Verify the certificate details or use another certificate.
512	Failed to sync asset to the following DWS servers: xxxx.	Reconfigure using the appropriate image. Supported image formats are .jpg, .png, and .bmp.
513	The customization has already been installed on DWS server: xxxx.	
514	Failed to apply customization on DWS server: xxxx.	Verify assets and workflows configuration for the device configuration.
515	Failed to remove customization on DWS server: xxxx.	Verify the device configuration and try again.
516	Failed to sync workflow to the following DWS server:xxxx.	Verify the workflows selected in the device configuration and try installing again.